(19)日本国特許庁(JP)

(12)公開特許公報(A)

(11)特許出願公開番号
特開2004-86441
(P2004-86441A)

(43)公開日 平成16年3月18日(2004.3.18)

| (51)Int.Cl.[7] | F I | | | テーマコード（参考） |
|---|---|---|---|---|
| G06F 15/00 | G06F | 15/00 | 330Z | 5B085 |
| G06F 17/60 | G06F | 15/00 | 330D | 5K067 |
| H04B 7/26 | G06F | 17/60 | 326 | |
| H04Q 7/20 | G06F | 17/60 | 506 | |
| | G06F | 17/60 | 512 | |

審査請求 有 請求項の数 10 OL （全 15 頁） 最終頁に続く

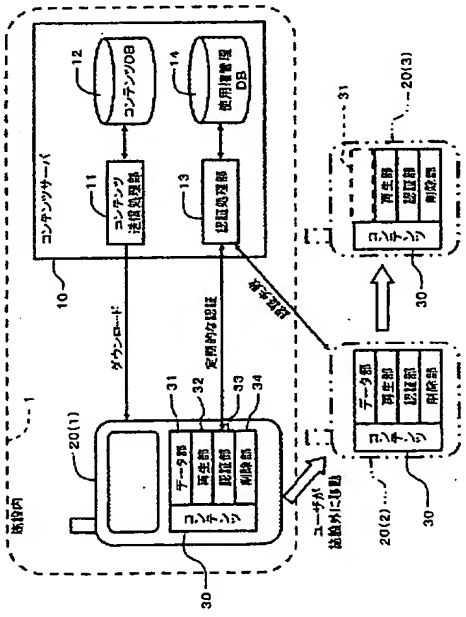
(21)出願番号 特願2002-245061(P2002-245061)
(22)出願日 平成14年8月26日(2002.8.26)

(71)出願人 000102728
株式会社エヌ・ティ・ティ・データ
東京都江東区豊洲三丁目３番３号
(74)代理人 100095371
弁理士 上村 輝之
(72)発明者 藤原 仁
東京都江東区豊洲三丁目３番３号 株式会社エヌ・ティ・ティ・データ内
(72)発明者 吉野 順
東京都江東区豊洲三丁目３番３号 株式会社エヌ・ティ・ティ・データ内

Fターム(参考) 5B085 AA08 BG02 BG03 BG07
5K067 AA21 BB04 BB21 DD43 GG22
HH22 JJ43 JJ52

(54)【発明の名称】コンテンツ管理システム

(57)【要約】
【課題】所定の圏内に位置する情報端末でのみコンテンツデータの閲覧や試聴を許可できるようにすること。
【解決手段】店舗や図書館あるいは学校等の施設１内に位置するユーザは、自分の情報端末２０内にサーバ１０からダウンロードしたコンテンツデータ３０を格納する。コンテンツデータ３０中の認証部３３は、サーバ１０との間で定期的な認証を行う。認証が失敗した場合は、端末２０が施設１外に出たものと判定され、端末２０に格納されたコンテンツデータの全部又は一部が削除され、その利用が禁止される。



1

【特許請求の範囲】
【請求項１】
コンテンツデータを管理するコンテンツ管理装置からユーザの情報端末に供給されるコンテンツデータを管理するコンテンツ管理システムにおいて、
前記情報端末が前記コンテンツ管理装置と通信可能な圏内に位置するか否かを判定する判定手段と、
前記判定手段により前記情報端末が前記圏内に位置すると判定された場合は、前記情報端末に供給された前記コンテンツデータの利用を許可し、前記判定手段により前記情報端末が前記圏外に位置すると判定された場合は、前記情報端末に供給された前記コンテンツデータの利用を禁止させる制御手段と、
を備えたことを特徴とするコンテンツ管理システム。
【請求項２】
前記判定手段は、前記情報端末と前記コンテンツ管理装置との間で定期的な通信を行わせ、予定された通信が正常に完了したか否かを検出することにより、前記判定を行うものである請求項１に記載のコンテンツ管理システム。
【請求項３】
前記制御手段は、前記情報端末が前記圏外に位置すると判定された場合は、前記情報端末に供給された前記コンテンツデータの全部又は一部を削除することにより、前記コンテンツデータの利用を禁止させるものである請求項２に記載のコンテンツ管理システム。
【請求項４】
前記制御手段は、前記情報端末が前記圏外に位置すると判定された場合、前記情報端末が前記コンテンツデータを再生中であるか否かを検査し、前記コンテンツデータの再生中である場合は、当該再生が終了した後で、前記コンテンツデータの利用を禁止させるものである請求項３に記載のコンテンツ管理システム。
【請求項５】
前記判定手段及び前記制御手段は、前記情報端末内で実行されるものである請求項４に記載のコンテンツ管理システム。
【請求項６】
前記判定手段及び前記制御手段は、前記コンテンツデータ内に予め設けられており、前記コンテンツデータが前記情報端末内に格納されることにより、それぞれ実行されるものである請求項５に記載のコンテンツ管理システム。
【請求項７】
前記情報端末と前記コンテンツ管理装置とは、近距離無線ＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）を介して双方向通信が可能である請求項６に記載のコンテンツ管理システム。
【請求項８】
前記コンテンツデータは、前記近距離無線ＬＡＮを介して前記情報端末に送信され、前記情報端末内に格納されるものである請求項７に記載のコンテンツ管理システム。

2

【請求項９】
前記コンテンツデータは、記録媒体を介して前記情報端末に供給されるものである請求項７に記載のコンテンツ管理システム。
【請求項１０】
コンテンツ管理装置からユーザの情報端末に供給されるコンテンツデータを管理するためのプログラムであって、
前記コンテンツデータを復号化して再生させる機能と、
前記情報端末が前記通信ネットワークを介して前記コンテンツ管理装置と通信可能な圏内に位置するか否かを判定する判定機能と、
前記情報端末が前記圏内に位置すると判定された場合は、前記コンテンツデータの利用を許可し、前記情報端末が前記圏外に位置すると判定された場合は、前記コンテンツデータの利用を禁止させる機能と、
をコンピュータ上で実現させるためのプログラム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、例えば、図書館、書店、音楽ＣＤ店、レンタルビデオ店等の各種施設内で映像データ等のコンテンツデータをユーザの情報端末に供給して試聴等させることができるコンテンツ管理システムに関する。
【０００２】
【従来の技術】
コンピュータ技術及びネットワーク技術の進展に伴い、例えば、書籍、映画、音楽等の各種コンテンツが、文字データ、静止画像データ、動画像データ、音楽データ等としてディジタル化されている。これらディジタル化されたコンテンツは、例えば、通信ネットワークを介して端末に配信されたり、ＤＶＤ－ＲＯＭ等の記録媒体に固定されて配布等されている。
【０００３】
ディジタル化されたコンテンツは、例えばインターネット等の通信ネットワークを介して容易にユーザの端末に配信することができる。従って、ネットワーク上の仮想店舗でディジタルコンテンツを販売することが可能であり、仮想店舗によるコンテンツデータの販売は急速に普及している。
【０００４】
ここで、サーバからコンテンツデータを配信する方式としては、ダウンロード方式とストリーミング方式とが知られている。ダウンロード方式は、コンテンツデータの全体を端末の記憶装置に格納させてから再生させるものであり、蓄積型の配信方法である。これに対し、ストリーミング方式は、非蓄積型の配信方法であり、端末は、

小分けされたコンテンツデータのブロックを受信しながら再生を開始し、再生済みのデータを破棄していくものである。

【０００５】

ダウンロード方式では、コンテンツデータの全体を端末の記憶装置に格納させるため、格納完了までの待ち時間が生じる。しかし、いったん保存したコンテンツは、特に制限を受けない限り、何度でも再生して楽しむことができる。一方、ストリーミング方式の場合は、再生開始までの待ち時間を最小に抑えることができるが、再生済みのデータを次々に破棄していくため、何度も繰り返して再生する場合は、その度にサーバにアクセスしてコンテンツデータを受信しなければならない。

【０００６】

【発明が解決しようとする課題】

上述の通り、ディジタル化されたコンテンツは、コンピュータ通信と馴染みやすく、仮想店舗を通じた販売等が行われやすい。しかし、ディジタル化されたコンテンツの全てがネットワークを介して無店舗で貸与されたり販売等されたりするわけではなく、現実の店舗等の施設内で、ディジタルコンテンツが販売されたり貸与される場合も考えられる。例えば、図書館内のＬＡＮを介して端末に書籍や映像のコンテンツデータを配信し、館内のユーザに閲覧させたり、あるいは、本屋や音楽ＣＤ店等で、商品である書籍や音楽のコンテンツデータを端末に配信して試聴させたりするような場合である。なお、コンテンツデータは、施設内のＬＡＮを介して供給される場合に限らず、ＣＤ－ＲＯＭやＤＶＤ－ＲＯＭ等の記録媒体を介してユーザに供給されることもある。

【０００７】

このように実際の施設内でディジタルコンテンツを配信するには、端末に配信したコンテンツデータの管理が特に重要となる。ディジタルデータは、コピーが容易で、コピーとオリジナルとの品質的な差もないためである。

【０００８】

そこで、１つの方法として、施設内にディジタルコンテンツ再生用の専用端末を設置し、専用端末を介してユーザに試聴や閲覧等させることが考えられる。専用端末であるため、端末内のコンテンツデータをユーザが無断で持ち出すことは通常不可能であり、データ管理の点からは優れている。しかしその反面、専用端末は一般に汎用の端末より高価なため、初期費用や維持費用等がかさむ。また、専用端末の設置台数が少ない場合は、多数のユーザに同時に試聴等させることができず、ユーザの待ち時間が増大して、顧客満足度が低下する。逆に、専用端末を予め十分多く設置すると、費用がかさむ上に、ユーザ数の少ない時間帯等では専用端末の稼働率が低下する。つまり、専用端末方式は、需要の変化に柔軟に対応することができず、費用面で問題を抱える。

【０００９】



他の方法として、パーソナルコンピュータやＰＤＡ（Ｐｅｒｓｏｎａｌ　Ｄｉｇｉｔａｌ　Ａｓｓｉｓｔａｎｔ）等の汎用の端末を採用し、汎用端末に施設内のサーバからＬＡＮを介してコンテンツデータを配信することも考えられる。汎用端末方式では、ユーザが持ち込んだ汎用端末を利用することもできるため、専用端末方式よりも費用面で大幅に有利である。しかし反面、ユーザが持参した汎用端末にコンテンツデータを保存して試聴や閲覧等を行わせることも可能なため、コンテンツデータの管理が難しく、施設外にコンテンツデータを持ち出されてしまう可能性がある。

【００１０】

そこで、コンテンツデータの再生回数や再生可能時期を予めコンテンツデータ内に設定しておくことにより、ユーザの汎用端末に保存されたコンテンツデータを管理する方法も考えられる。再生回数や再生可能時期の制限により、コンテンツデータをある程度管理することができる。

【００１１】

しかし、再生回数や再生可能時期という条件自体は、そのコンテンツデータを供給した施設（図書館や店舗等）との関連性が無い。従って、例えば、施設を訪れたユーザのみにコンテンツデータの試聴等を許可したい場合や、施設内での販売に結びつけるために試聴等を許可したい場合等のような要求に応えることができないという問題がある。つまり、施設の運営者がその施設内でのみコンテンツデータの供給を行いたい場合には、従来の方法はそのまま採用できない。

【００１２】

本発明は、上記の課題に鑑みてなされたものであり、その目的は、所定の圏内でのみコンテンツデータを利用できるようにしたコンテンツ管理システムを提供することにある。本発明の他の目的は、後述する実施の形態の記載から明らかになるであろう。

【００１３】

【課題を解決するための手段】

上記課題を解決するため、本発明に係るコンテンツ管理システムは、コンテンツ管理装置からユーザの情報端末に供給されるコンテンツデータを管理するものであって、判定手段と制御手段とを備えている。

【００１４】

判定手段は、情報端末がコンテンツ管理装置と通信可能な圏内に位置するか否かを判定する。制御手段は、判定手段により情報端末が圏内に位置すると判定された場合は、情報端末に供給されたコンテンツデータの利用を許可し、判定手段により情報端末が圏外に位置すると判定された場合は、情報端末に供給されたコンテンツデータの利用を禁止させる。

【００１５】

ここで、「コンテンツ管理装置」は、例えば、図書館、

学校、コンビニエンスストアや量販店等の各種店舗、駅、空港、銀行、病院、ホテル、行政庁舎等の施設内又は施設に関連づけられて設けられる。具体的には、コンテンツ管理装置を各施設内にそれぞれ設置してもよいし、あるいは、１台又は複数台のサーバで１カ所又は複数箇所の施設にコンテンツデータを送信する等のように、施設外に設置したコンテンツ管理装置によりコンテンツデータを管理してもよい。情報端末とコンテンツ管理装置は、通信ネットワークを介して双方向通信を行うことができる。通信ネットワークとしては、例えば、ＬＡＮや移動体通信を挙げることができる。ＬＡＮは、有線接続、無線接続どちらでもよい。「情報端末とサーバとが通信可能な圏内」は、例えば、壁や家具等の配置、無線ＬＡＮアクセスポイントやハブの設置場所等によっても相違するが、施設の建物又は敷地とほぼ一致する場合のほか、建物や敷地内の一部でのみ通信可能な場合、通信可能な圏内が建物や敷地の外部に及ぶ場合もある。「コンテンツデータ」としては、例えば、書籍、音楽、映画、ドラマ、ニュース、テレビジョン番組、ラジオ番組等を挙げることができる。

【００１６】

制御手段は、情報端末が所定の圏内にある場合にコンテンツデータの利用を許可し、情報端末が圏外に出た場合はコンテンツデータの利用を禁止させる。これにより、施設と関連づけて、ユーザにコンテンツデータを利用させることができる。ここで、コンテンツデータは、情報端末の記憶装置（メモリやハードディスク装置等）にいったん保存されるが、コンテンツデータの配信に際しては、いわゆるストリーミング方式を採用し、受信した部分から直ちに再生するようにしてもよい。あるいは、コンテンツデータは記録媒体に記録された状態で、情報端末に供給される場合もある。

【００１７】

本発明の一態様では、判定手段は、情報端末とコンテンツ管理装置との間で定期的な通信を行わせ、予定された通信が正常に完了したか否かを検出することにより、判定を行うようになっている。

【００１８】

コンテンツ管理装置と情報端末との間で定期的な通信を行わせることにより、２つのコンピュータ間での接続が維持されているか否かに基づいて、情報端末が所定の圏内にあるか否かを判定することができる。

【００１９】

本発明の一態様では、制御手段は、情報端末が圏外に位置すると判定された場合は、情報端末に供給されたコンテンツデータの全部又は一部を削除することにより、コンテンツデータの利用を禁止させる。

【００２０】

コンテンツデータの全体を削除してしまえば、その後コンテンツデータを利用することはできなくなる。あるいは、コンテンツデータが暗号化されている場合に復号化キーのデータのみを削除する等のように、コンテンツデータの一部を削除するだけでも、コンテンツデータの利用を禁止させることができる。さらに、コンテンツデータの全体からランダムに又は所定の規則の下にデータを間引きすることにより、コンテンツデータの利用を禁止してもよい。コンテンツデータの一部を削除する場合は、削除部分のみを情報端末が再取得することにより、コンテンツデータを再利用できるため、再利用時のデータ受信時間を短縮することができる。



【００２１】

本発明の一態様では、制御手段は、情報端末が圏外に位置すると判定された場合、情報端末がコンテンツデータを再生中であるか否かを検査し、コンテンツデータの再生中である場合は、当該再生が終了した後で、コンテンツデータの利用を禁止させる。

【００２２】

例えば、情報端末でコンテンツデータを再生中のユーザが、所用で一時的に圏外に出たような場合に、直ちにコンテンツデータの利用を禁止せず、現在の再生が終了するまで猶予を与える。

【００２３】

判定手段及び制御手段は、情報端末内で実行することができる。

【００２４】

さらに、判定手段及び制御手段は、コンテンツデータ内に予め設けられており、コンテンツデータが情報端末内に格納されることにより、それぞれ実行されるように構成することができる。

【００２５】

即ち、判定手段及び制御手段をコンピュータプログラムとして構成し、このプログラムをコンテンツデータ内に含めて情報端末に供給し、情報端末内で実行させる。

【００２６】

なお、コンテンツデータは、近距離無線ＬＡＮ又は記録媒体を介して情報端末に供給することができる。あるいは、コンテンツデータの一部は無線ＬＡＮを介して情報端末に供給し、残りのコンテンツデータは記録媒体を介して情報端末に供給する場合もあり得る。

【００２７】

本発明は、コンピュータプログラムの発明として把握することもでき、コンピュータプログラムは、例えば、ＣＤ－ＲＯＭ、ＤＶＤ－ＲＯＭ、メモリ、ハードディスク、磁気テープ等の記録媒体に記録して配布できるほか、通信ネットワークを介しても配信することができる。

【００２８】

【発明の実施の形態】

以下、図１～図８に基づき本発明の実施の形態について詳述する。

7

【００２９】

１．第１の実施の形態

【００３０】

まず、図１～図６は本発明の第１の実施の形態に係る。図１は、コンテンツ管理システムの全体概要を示す機能ブロック図であって、例えば、図書館や店舗等の施設１には、コンテンツサーバ１０（以下、「サーバ１０」と略記）が設けられており、施設内のユーザは、自分の情報端末２０にサーバ１０から送信されたコンテンツデータを保存して再生することにより、コンテンツの試用（一時的限定的な視聴等）が行えるようになっている。以下、施設１の一例として、書籍や音楽ディスクの販売を行う店舗を例に説明する。

【００３１】

サーバ１０は、コンテンツ送信処理部１１，コンテンツデータベース（図中では「ＤＢ」と略記）１２，認証処理部１３及び使用権管理データベース１４を備えている。なお、サーバ１０は、各施設１のそれぞれに個別に設置することもできるし、あるいは、本店や本部等の施設１の外部に設置したサーバ１０によって、複数の支店や加盟店等でコンテンツデータの配信サービスをそれぞれ行うようにすることもできる。また、サーバ１０は、１台のコンピュータから構成される必要はなく、複数のコンピュータを連係動作させて構成してもよい。

【００３２】

コンテンツ送信処理部１１は、情報端末２０からの要求に応じたコンテンツデータ又は予め設定されたコンテンツデータを、コンテンツデータベース１２から読出し、ハブや無線ＬＡＮアクセスポイント等を介して、情報端末２０に送信するものである。例えば、キャンペーン中のコンテンツの場合は、情報端末２０からの要求の有無を問わずにコンテンツデータを送信するように構成することができ、この場合、ユーザの同意を得るのが望ましいが、これに限らず、場合によっては、ユーザの同意を確認する前に、又はユーザの同意を得ることなく、コンテンツデータを送信する構成としてもよい。

【００３３】

認証処理部１３は、後述する情報端末２０側からの要求に応じて、認証処理を行うものである。本実施の形態では、後述のように、ユーザ認証（正当な権限を有するユーザであるか否かの認証）、端末認証（正当な権限を有する端末であるか否かの認証）及び端末位置認証（所定のエリアに端末が位置するか否かの認証であり、エリア認証と呼ぶこともできる）の３種類の認証を行っている点に留意すべきである。コンテンツデータベース１２及び使用権管理データベース１４については、図３と共に後述する。

【００３４】

ユーザが所持する情報端末２０は、例えば、パーソナルコンピュータ、ＰＤＡ、携帯電話、音楽プレイヤー、デ

8

ィジタルカメラ、ディジタルビデオカメラ等として実現されるものである。即ち、情報端末２０は、コンテンツデータを記憶する記憶機能、コンテンツデータの再生処理等のデータ処理を行うデータ処理機能、サーバ１０との間で双方向のデータ通信を行う通信機能、再生されたコンテンツデータを視覚や聴覚等でユーザに提供するユーザインターフェース機能を備えていればよい。また、情報端末２０は、ユーザの所有物である必要はなく、施設１側から貸与されるものでもよい。

【００３５】

情報端末２０は、サーバ１０から受信したコンテンツデータ３０を保存して再生する。コンテンツデータ３０は、文字データや音楽データあるいは画像データ等からなるデータ部３１と、データ部３１を再生するための再生部３２と、サーバ１０との間で認証を行うための認証部３３と、コンテンツデータ３０の全体又は復号化キーデータのみを削除するための削除部３４とを備えている。再生部３２，認証部３３及び削除部３４は、情報端末２０内にダウンロードされ、情報端末の演算処理装置により実行されるプログラムである。

【００３６】

図１中に「情報端末２０（１）」として示すように、情報端末２０を所持するユーザが施設１内に居る間は、情報端末２０の認証部３３とサーバ１０の認証処理部１３との間で定期的な認証が行われる。この認証が成功している間は、情報端末２０がサーバ１０との交信エリア内に存在するものと判定され、再生部３２はデータ部３１を再生する。「情報端末２０（２）」として示すように、ユーザが施設１の外部に出て、サーバ１０との交信エリア外に移動すると、移動後に行われる最初の認証が失敗する。

【００３７】

これにより、情報端末２０が交信エリア外に出たことを認証部３３が検出し、「情報端末２０（３）」として示すように、削除部３４がコンテンツデータ３０の全体を、又はデータ部３１の再生に必要な復号化キーデータを削除する。なお、説明の便宜上、図１中では、データ部３１のみを削除するかのように示しているが、本発明はこれに限定されない。交信エリア外におけるコンテンツデータの再生を禁止することができるように、コンテンツデータ３０の全部又は一部を削除すればよい。さらに、一部を削除する場合としては、復号化キーデータの削除、データ本体であるデータ部３１の全部削除、データ部３１の部分的な削除等を行うことができる。

【００３８】

図２は、コンテンツデータ３０及びライセンス４０の関係を示す説明図であり、ディジタル化されたコンテンツデータ３０は、一意に割り当てられた識別情報としてのコンテンツＩＤ（ＩＤｅｎｔｉｔｙ）を有する。また、データ部３１は所定の暗号アルゴリズムに基づいて暗号

9

化されており、その復号化のためには、ライセンス４０に含まれる復号化キーデータが必要とされる。

【００３９】

ライセンス４０は、コンテンツデータ３０を再生するために必要なデータである。ライセンス４０には、コンテンツデータ３０との対応関係を示すコンテンツＩＤと、データ部３１を復号化するためのキーデータと、コンテンツを再生するための条件とを含めることができる。

【００４０】

コンテンツ再生条件としては、例えば、再生可能回数、再生可能期間、視聴可能なページ数等を挙げることができる。これらのコンテンツ再生条件は、例えば、コンテンツのカテゴリー（音楽か書籍か等）、コンテンツのジャンル（音楽カテゴリー内の場合、軽音楽かクラシックか等）、コンテンツのデータサイズ、コンテンツ制作者やコンテンツ販売者の意向（例えば、キャンペーン期間中は試聴回数を増加させる等）に応じて、設定することができる。また、同一のコンテンツデータであっても、試用するユーザ毎にコンテンツ再生条件を設定することも可能である。例えば、その店舗での購入金額が多いユーザや、コンテンツがターゲットとする顧客層に属するユーザには、一般ユーザよりも長時間の試聴を許可することが可能である。

【００４１】

図３は、コンテンツデータベース１２及び使用権管理データベース１４の記憶内容の一例を示す説明図である。

【００４２】

図３（ａ）に示すコンテンツテーブル４１は、コンテンツデータベース１２に設けられるもので、例えば、コンテンツＩＤ、コンテンツの格納位置を示すパス（格納先アドレス）、コンテンツの説明、著作権管理情報、コンテンツの属するカテゴリ等を対応付けて管理している。

【００４３】

次に、図３（ｂ）～（ｇ）は、使用権管理データベース１４に記憶されるものであり、図３（ｂ）に示すコンテンツ使用権管理テーブル４２は、例えば、コンテンツＩＤ、復号キーデータ、試用可否フラグ、コンテンツ価格等を対応付けて管理している。試用可否フラグは、そのコンテンツの試用が許可されているか否かを示す情報である。

【００４４】

図３（ｃ）に示すユーザ管理テーブル４３は、例えば、各ユーザ毎に一意に割り振られたユーザＩＤとユーザ情報とを対応付けて管理している。ユーザ情報としては、例えば、ユーザの氏名、住所、電話番号、電子メールアドレス、職業、家族構成、趣味、過去の購入履歴等を挙げることができる。

【００４５】

図３（ｄ）に示す端末管理テーブル４４は、例えば、各情報端末２０毎に一意に割り当てられた端末ＩＤと端末

10

情報とを対応付けて管理している。端末情報としては、例えば、情報端末の種類（携帯電話かパーソナルコンピュータか）、製造メーカー名、機種名、データ処理能力（ＣＰＵ、メモリ量、搭載ＯＳの種類等）、データ通信能力（通信速度等）、ユーザインターフェースの能力（カラーディスプレイ搭載かモノクロディスプレイか等）を挙げることができる。

【００４６】

図３（ｅ）に示すコンテンツ使用条件管理テーブル４５は、例えば、コンテンツＩＤとコンテンツ再生条件とを対応付けて管理している。コンテンツ再生条件の具体例は、上述した通りである。

【００４７】

図３（ｆ）に示すコンテンツ購入管理テーブル４６は、例えば、ユーザＩＤとコンテンツＩＤと再生フラグとを対応付けて管理している。再生フラグは、コンテンツＩＤで特定されるコンテンツデータが現在再生中であるか否かを示す情報である。

【００４８】

図３（ｇ）に示す端末位置管理テーブル４７は、例えば、エリア情報とエリアの詳細情報とを対応付けて管理している。エリア情報とは、サーバ１０との交信可能エリアを特定する位置情報であり、例えば、交信可能エリアの住所、緯度経度等である。エリア情報により、情報端末２０がサーバ１０と交信可能な地域的範囲を知ることができる。また、エリアの詳細情報とは、サーバ１０と情報端末２０とが交信可能なエリアの詳細を記すもので、例えば、施設名称、施設管理者名、施設の構造（何階建てか等）、交信エリア内の交信不能場所（壁や家具、アクセスポイントの配置等により交信不能な場所がある場合）等を挙げることができる。

【００４９】

次に、図４～図６に基づき、本実施の形態による各部の動作を説明する。以下、ステップを「Ｓ」と略記する。また、図に示すフローチャートは、処理動作の概要を示すものであって、実際のプログラムとは相違する場合がある。

【００５０】

図４は、情報端末２０に保存されたコンテンツデータ３０の再生部３２による再生処理のフローチャートである。

【００５１】

まず、使用権管理データベース１４を検索することにより、再生しようとするコンテンツデータが既に購入済みであるか否かを判定する（Ｓ１）。コンテンツデータがまだ購入されていない場合は（Ｓ１：ＮＯ）、再生が許可されている端末であるか否かを判定する（Ｓ２）。例えば、予め施設１内に設置された端末や施設１側がユーザに貸与した端末かユーザが持ち込んだ私物であるかを検査する。

11

【００５２】
ユーザが施設１内に持ち込んだ私物の端末の場合は（Ｓ２：ＮＯ）、コンテンツの再生が許可されたエリア内に情報端末２０が位置するか否かを判定する（Ｓ３）。図５に示す定期的に行われる認証処理が成功している間は、許可されたエリア内に位置するものとして判定される。

【００５３】
このように、本実施の形態では、購入したユーザであるか否かのユーザ認証（Ｓ１）、再生権限を有する情報端末であるか否かの端末認証（Ｓ２）に加えて、交信可能エリア内に位置する端末であるか否かという端末位置認証又はエリア認証（Ｓ３）が行われる。

【００５４】
コンテンツデータが購入されていない場合でも、再生が許可された情報端末２０である場合（Ｓ２：ＹＥＳ）又は交信エリア内に位置する情報端末２０である場合（Ｓ３：ＹＥＳ）は、試用モードに以降し、ライセンスが発行される（Ｓ５）。そして、ライセンスが発行されて再生が開始されたことを使用権管理データベース１４に反映させ（Ｓ６）、コンテンツデータを復号化して再生する（Ｓ７）。

【００５５】
そして、コンテンツデータ３０に設定されている再生条件が許す範囲内で、コンテンツデータを再生する（Ｓ８）。例えば、５分間のみ試聴可、３ページだけ閲覧可等のように、予め許可された範囲内での再生が行われるまで再生部３２は待機し、許可された範囲内での再生が行われた場合は（Ｓ８：ＹＥＳ）、ライセンスを削除し（Ｓ９）、再生が完了したことを使用権管理データベース１４に反映させる（Ｓ１０）。

【００５６】
一方、購入済みのユーザである場合は（Ｓ１：ＹＥＳ）、コンテンツデータ購入時に使用した情報端末であるか否かを判定する（Ｓ１１）。コンテンツデータの購入時とコンテンツデータの再生時の情報端末２０が一致している場合は（Ｓ１１：ＮＯ）、ライセンスを発行する（Ｓ５）。

【００５７】
また、過去にそのコンテンツデータを購入したユーザであっても、他の情報端末２０で新たに再生しようとする場合は（Ｓ１１：ＹＥＳ）、コンテンツ購入処理に移行し、再度のコンテンツ購入を促す（Ｓ４）。但し、これは、コンテンツ利用権を端末毎に販売する場合であって、端末の種類を問わずに一度購入したコンテンツデータの自由な利用を認めるような場合には、Ｓ１１を省略し、購入済みユーザであると判断された場合は、ライセンスを発行させてもよい。

【００５８】
なお、コンテンツデータが未購入であり（Ｓ１：ＮＯ）、予め再生が許可されている端末でもなく（Ｓ２：ＮＯ）、さらに、情報端末２０が所定の交信エリア内に位置していない場合は（Ｓ３：ＮＯ）、ユーザにコンテンツデータの購入を促す（Ｓ４）。

12

【００５９】
コンテンツデータの購入処理では、例えば、購入しようとするコンテンツをユーザが明示的に指定し、クレジットカード決済、電子マネー決済、銀行振込等の決済方法を選択し、所定の個人情報を入力することにより完了する。

【００６０】
次に、図５は、コンテンツデータ３０の認証部３３により実行される認証処理のフローチャートである。

【００６１】
コンテンツデータ３０がユーザの情報端末２０にダウンロードされると、認証部３３は自動的に起動する（Ｓ２１）。認証部２２は、ライセンスをサーバ１０から情報端末２０にダウンロードさせた後（Ｓ２２）、サーバ１０の認証処理部１３との間で所定の認証を行う（Ｓ２３）。認証処理が成功した場合は、所定の時間待ちを行い（Ｓ２５）、所定の時間が経過した時は再度ライセンスをダウンロードし（Ｓ２２）、サーバ１０との間で認証を行う（Ｓ２３，Ｓ２４）。

【００６２】
ユーザの情報端末２０がサーバ１０と交信可能な圏内に位置する間は、情報端末２０とサーバ１０との間で正常に認証処理が行われるが、ユーザの情報端末２０が交信可能圏外に移動した場合は、サーバ１０と情報端末２０との間で通信を行うことができないため、認証処理が失敗する（Ｓ２４：ＮＯ）。

【００６３】
情報端末２０とサーバ１０との間で通信が行えず、認証が失敗した場合は、削除部３４に予め設定されている削除フラグの内容を検査する（Ｓ２６）。削除フラグは、情報端末２０でのコンテンツデータの再生を禁止するモードを指定する情報であり、本実施の形態では、認証失敗後に直ちに削除する第１の削除モードと、認証失敗後に現在の再生終了を待ってから削除する第２のモードとを用意してある。

【００６４】
認証部３３は、削除フラグによって指定された削除モードが第１のモードか第２のモードかを判定し（Ｓ２７）、再生終了を待ってから削除する第２のモードを指定されている場合は（Ｓ２７：ＹＥＳ）、コンテンツデータ３０が再生中か否かを判定する（Ｓ２８）。再生中である場合は、現在の再生が完了するまで時間待ちを行う（Ｓ２９）。ここで、コンテンツデータ３０全体の再生が完了するのを待たずに、コンテンツデータ３０のうち一部分の再生完了を待ってから削除するようにしてもよい。例えば、複数の独立した短編から構成されている

13

書籍コンテンツや複数の独立した楽曲データから構成されている音楽コンテンツの場合等には、現在閲覧中又は試聴中の部分の再生を完了した後で削除し、他の未読部分又は未試聴部分の閲覧を禁止するようにしてもよい。

【００６５】

コンテンツデータ３０の再生が完了した場合（Ｓ２８：ＮＯ）又は認証失敗後に直ちに削除する第１の削除モードが指定されていた場合（Ｓ２７：ＮＯ）は、認証部３３は、ライセンスを破棄し（Ｓ３０）、削除部３４を起動させる（Ｓ３１）。

【００６６】

図６は、削除部３４により実行される削除処理を示すフローチャートである。認証部３３によって削除部３４が起動されると、削除部３４は、コンテンツデータ３０の全体を削除するためのプログラム（例えばスクリプト）を生成し、カレントディレクトリに配置する（Ｓ４１）。

【００６７】

次に、削除部３４は、削除プログラムを起動させ（Ｓ４２）、削除部自身の実行を終了する（Ｓ４３）。

【００６８】

このようにして削除部３４により起動された削除プログラムは、削除部３４の起動状態を確認し（Ｓ５１）、削除部３４の起動が終了するまで待機する（Ｓ５２，Ｓ５３）。削除部３４の実行が終了すると（Ｓ５２：ＮＯ）、削除プログラムは、コンテンツデータ３０の全体を削除する（Ｓ５４）。

【００６９】

なお、認証が失敗した場合に、ライセンスが既に破棄されているため、コンテンツデータ３０を削除しなくても、その再生を行うことはできない。従って、交信エリア外に出た情報端末２０でのコンテンツの利用を阻止するという目的は既に達成されており、図６に示す削除処理は必ずしも必要ではない。

【００７０】

しかしながら、削除処理を行うことにより、不正な再使用をより強固に防止することができ、コンテンツ管理システムの信頼性が高まる。一方、ライセンスのみを削除し、コンテンツデータ３０を削除しない場合は、ライセンスのみを情報端末２０に再びダウンロードするだけで、コンテンツデータ３０を再度利用することができる。

【００７１】

このように構成される本実施の形態によれば、汎用の情報端末２０を用いてコンテンツデータの配信及び管理を行うことができるため、専用端末を用いる場合よりも安価かつ容易にシステムを構築することができる。特に、ストリーミング方式ではなく、情報端末２０内にコンテンツデータ３０の全体を予め格納させてから再生させるダウンロード方式を採用するため、サーバ１０を安価に

14

構築することができる。また、ネットワークトラフィックが変動した場合でもコンテンツ再生の質に影響がなく、安定した品質を提供できる。

【００７２】

また、ユーザが施設１の外部に移動した場合は、ユーザの情報端末２０に格納されたコンテンツデータ３０の再生を禁止するため、不正なコピーや改ざん等を未然に防止することができる。ディジタル化されたコンテンツデータは、従来の物理的媒体に依存する著作物とは異なり、複製や改ざん等が容易であるという特徴を有する。しかし、暗号化等の保護対策が適用されたコンテンツデータを不正にコピー等するには、特殊なソフトウェアや情報端末２０よりも処理能力の高いコンピュータ等を用いる必要がある。ユーザが携行する情報端末２０は、通常の場合、データ処理能力の低いコンピュータ装置であるから、施設１外へのコンテンツデータの持ち出しを未然に禁止するだけでも安全性が高まる。

【００７３】

さらに、ユーザの情報端末２０が施設１の内外いずれに位置するかによってコンテンツデータ３０の利用を制御することができるため、施設１外でのコンテンツ利用を制限したい場合等に有効である。例えば、学校等での講義にのみ使用するという条件で著作権者の了解を得てコンテンツデータを配信する場合に、講義外でのコンテンツデータの無断利用を未然に阻止することができる。従って、ディジタル化されたコンテンツデータの利用の可能性を広げることができる。

【００７４】

本発明を適用可能なビジネスモデルの例を幾つか列挙すると、例えば、音楽ディスク店や書店等では、来店したユーザの情報端末２０にユーザが希望する音楽や書籍のコンテンツデータ３０を配信して試聴や立ち読み等を許可させることができ、ユーザが店外に出た場合はコンテンツデータ３０の利用を禁止することができる。また、例えば、図書館や学校などでは、館内や学校内にいるユーザにのみコンテンツデータ３０の利用を許可することができる。

【００７５】

２．第２の実施の形態

【００７６】

次に、図７及び図８に基づいて本発明の第２の実施の形態を説明する。本実施の形態の特徴は、情報端末２０が位置特定機能（ＧＰＳ：Ｇｌｏｂａｌ　Ｐｏｓｉｔｉｏｎｉｎｇ　Ｓｙｓｔｅｍ）を内蔵又は外付けで利用可能な場合に、ＧＰＳにより得られた位置情報も利用して施設１の内外いずれに位置するかを判断する点にある。

【００７７】

図７に示すように、コンテンツデータ３０内には、情報端末２０のＧＰＳ機能を利用して位置情報を収集するＧＰＳ部３５が設けられている。

15

【００７８】
図８に示すように、認証部３３は、サーバ１０との認証が成功した場合に（Ｓ２４：ＹＥＳ）、ＧＰＳ部３５からの位置情報に基づいて、情報端末２０の現在位置が許可されたコンテンツ利用エリア内に位置するか否かを判定する（Ｓ６０）。サーバ１０との認証が成功した場合でも、情報端末２０が所定のエリア外に位置する場合は（Ｓ６０：ＮＯ）、上述の通り、コンテンツデータ３０の利用が禁止される（Ｓ２６～Ｓ３１）。

【００７９】
本実施の形態では、情報端末２０と施設１との位置関係を、サーバ１０と情報端末２０との間の通信による認証とＧＰＳ機能による位置情報とで２重に判定するため、施設外部でのコンテンツ利用をより一層効果的に阻止できる。

【００８０】
なお、本発明は、上述した実施の形態に限定されない。当業者であれば、前記各実施の形態に構成要素を追加したり、削除したり、変更等したりして種々の変形を行うことができる。

【００８１】
例えば、コンテンツサーバから無線ＬＡＮを介してコンテンツデータを情報端末に供給する場合に限らず、ＣＤ－ＲＯＭ、ＤＶＤ－ＲＯＭ、ＰＣカード、メモリ等の記録媒体を介して情報端末にコンテンツデータを供給するようにしてもよい。記録媒体を介して情報端末に供給されたコンテンツデータでも、上記実施の形態と同様に、コンテンツ管理装置と定期的又は不定期に交信し、情報端末の所在を確認してコンテンツデータの利用を制御することができる。

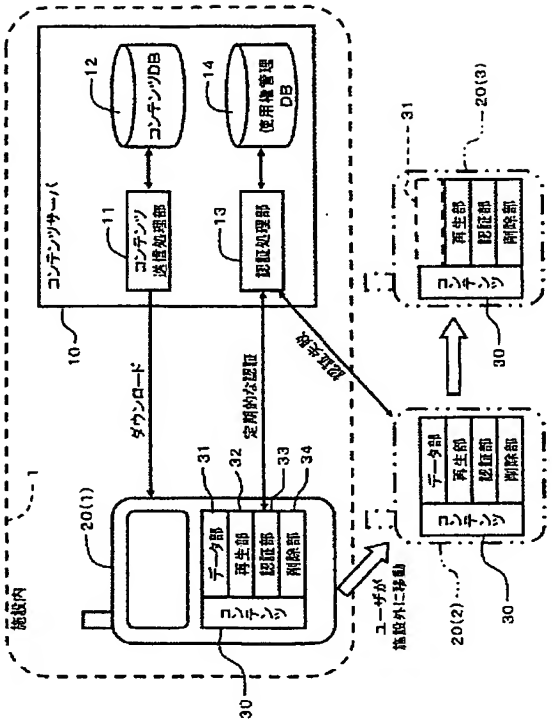
【００８２】
【発明の効果】

16

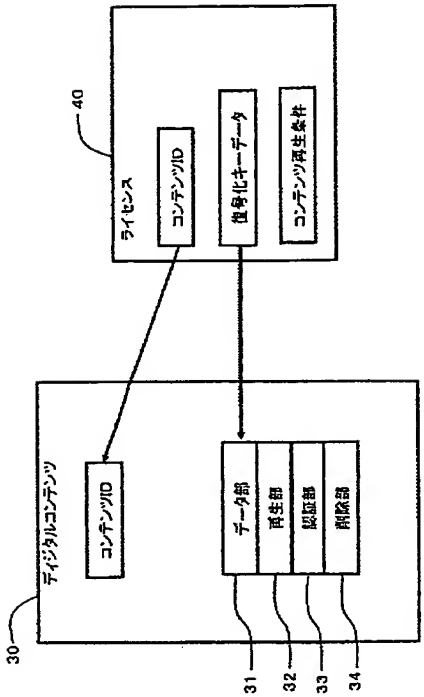
以上説明した通り、本発明に係るコンテンツ管理システムによれば、ユーザの情報端末が所定の圏内に位置する場合にコンテンツデータの利用を許可し、端末が圏外に出た場合はコンテンツデータの利用を禁止することができる。

【図面の簡単な説明】
【図１】本発明の第１の実施の形態に係るコンテンツ管理システムの全体構成を示すブロック図である。
【図２】コンテンツデータとライセンスとの関係を示す模式図である。
【図３】各データベースの記憶構造を示す説明図である。
【図４】再生処理を示すフローチャートである。
【図５】認証処理を示すフローチャートである。
【図６】削除処理を示すフローチャートである。
【図７】本発明の第２の実施の形態に係るコンテンツ管理システムの全体構成を示すブロック図である。
【図８】認証処理を示すフローチャートである。
【符号の説明】
１　施設
１０　コンテンツサーバ
１１　コンテンツ送信処理部
１２　コンテンツデータベース
１３　認証処理部
１４　使用権管理データベース
２０　情報端末
３０　コンテンツデータ
３１　データ部
３２　再生部
３３　認証部
３４　削除部
３５　ＧＰＳ部

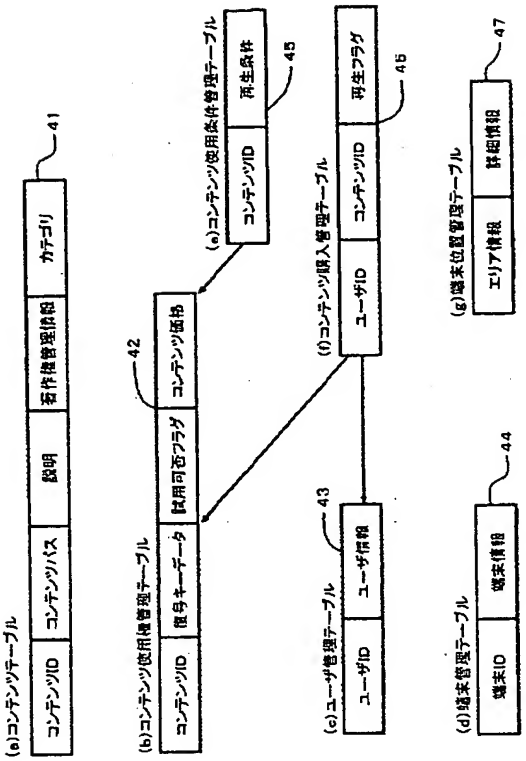
【図１】


施設内
1
コンテンツサーバ
10
12
コンテンツDB
14
使用権管理DB
11
コンテンツ送信処理部
13
認証処理部
ダウンロード
定期的な認証
要求取得
20(1)
31
32
33
34
データ部
再生部
認証部
削除部
コンテンツ
30
ユーザが施設外に移動
20(2)
20(3)

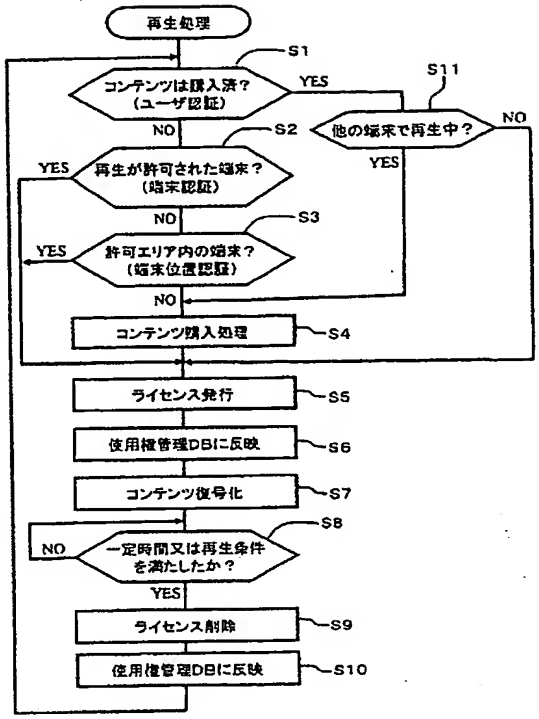
【図２】


40
ライセンス
コンテンツID
復号化キーデータ
コンテンツ再生条件
ディジタルコンテンツ
コンテンツID
データ部
再生部
認証部
削除部
30
31
32
33
34

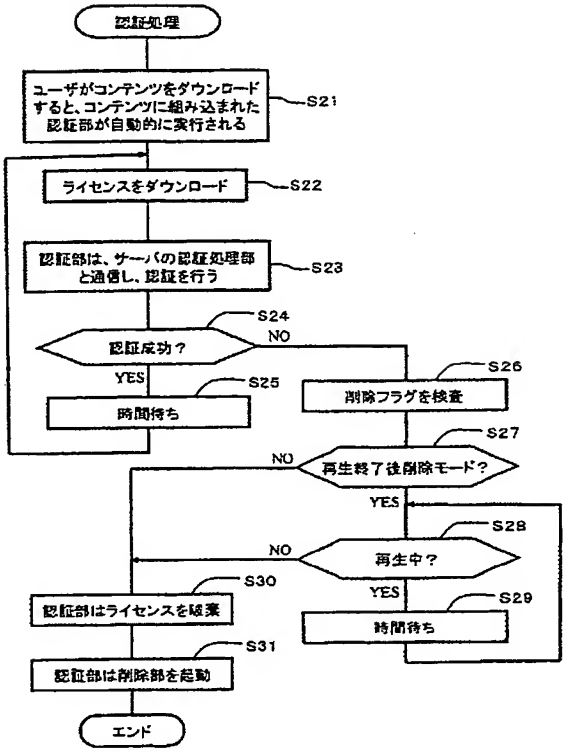
【図３】


(a)コンテンツテーブル
コンテンツID
コンテンツパス
説明
著作権管理情報
カテゴリ
41
(b)コンテンツ使用権管理テーブル
コンテンツID
復号キーデータ
使用可否フラグ
コンテンツ価格
42
(c)ユーザ管理テーブル
ユーザID
ユーザ情報
43
(d)端末管理テーブル
端末ID
端末情報
44
(e)コンテンツ使用条件管理テーブル
コンテンツID
再生条件
45
(f)コンテンツ購入管理テーブル
ユーザID
コンテンツID
再生フラグ
46
(g)端末位置管理テーブル
エリア情報
詳細情報
47

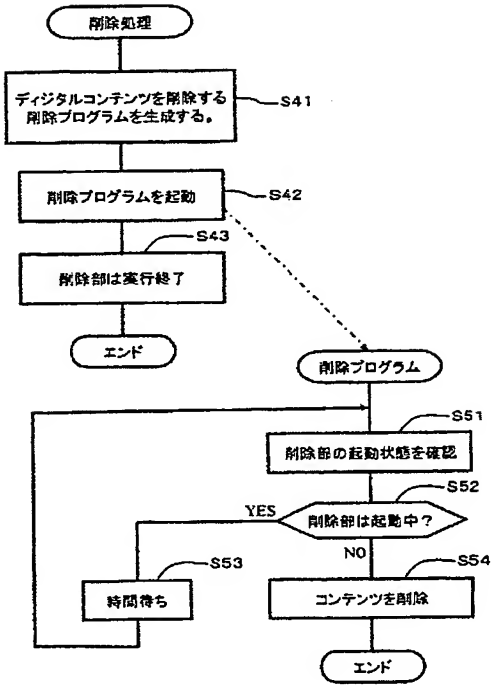
【図４】


再生処理
S1
コンテンツは購入済？
（ユーザ認証）
YES
S11
他の端末で再生中？
NO
YES
NO
S2
再生が許可された端末？
（端末認証）
YES
NO
S3
許可エリア内の端末？
（端末位置認証）
YES
NO
コンテンツ購入処理
S4
ライセンス発行
S5
使用権管理DBに反映
S6
コンテンツ復号化
S7
S8
NO
一定時間又は再生条件
を満たしたか？
YES
ライセンス削除
S9
使用権管理DBに反映
S10

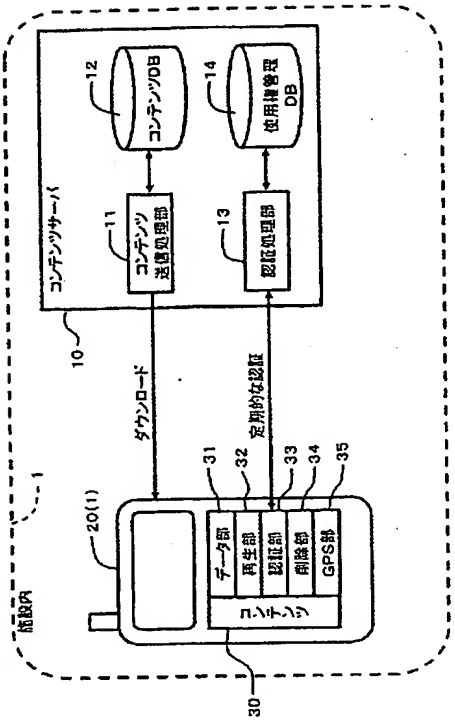
【図５】


認証処理
ユーザがコンテンツをダウンロードすると、コンテンツに組み込まれた認証部が自動的に実行される
S21
ライセンスをダウンロード
S22
認証部は、サーバの認証処理部と通信し、認証を行う
S23
S24
認証成功？
NO
YES
S25
時間待ち
S26
削除フラグを検査
S27
再生終了後削除モード？
NO
YES
S28
再生中？
NO
YES
S29
時間待ち
S30
認証部はライセンスを破棄
S31
認証部は削除部を起動
エンド

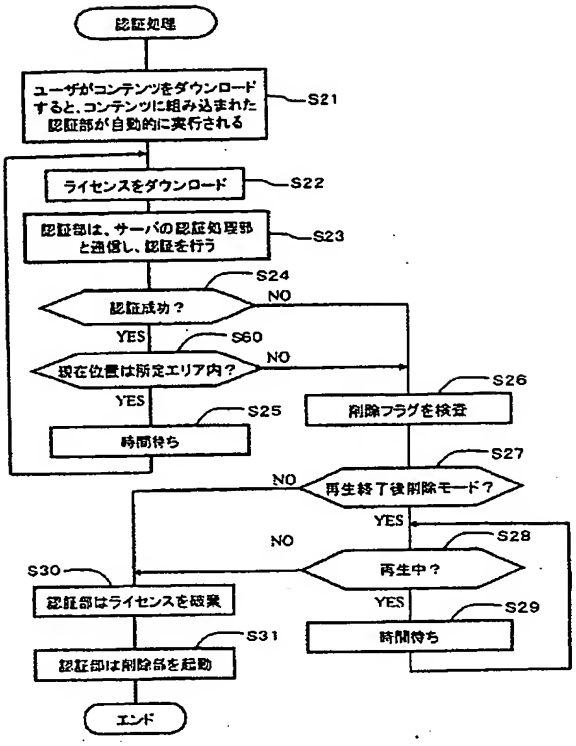
【図６】


削除処理
ディジタルコンテンツを削除する削除プログラムを生成する。
S41
削除プログラムを起動
S42
S43
削除部は実行終了
エンド
削除プログラム
S51
削除部の起動状態を確認
S52
YES
削除部は起動中？
NO
S53
時間待ち
S54
コンテンツを削除
エンド

【図７】




【図８】




フロントページの続き

| (51) Int. Cl.[7] | F I | | テーマコード（参考） |
|---|---|---|---|
| | Ｈ０４Ｑ 7/04 | Ｚ | |
| | Ｈ０４Ｂ 7/26 | Ｍ | |